UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/667,286	09/22/2000	Magda M. Mourad	(YOR920000599)13873	1205

7590 01/12/2005

Richard L Catania
Scully Scott Murphy & Presser
400 Garden City Plaza
Garden City, NY 11530

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/667,286	MOURAD ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07/06/2004 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09/22/2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 14-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Hurtado et al (US 6,611, 812 B2).

a. *Referring to claim 14:*

i. Hurtado teaches:

(1) a certificate generator for receiving applications, for determining if the applications exhibit a predefined property, and for issuing a trust certificate for each of the applications that exhibits the predefined property **[i.e., referring to Figure 1C, in the Secure Digital Content Electronic Distribution System 100, the Clearinghouse(s) 105, that is "a certificate generator", has the option of issuing certificates to the Electronic Digital Content Store(s) 163 (column 17, lines 42-45)]**;

(2) a certificate repository for receiving and storing trust certificates issued by the certificate generator **[i.e., referring to Figure 1B, electronic digital content store(s) 103 that is "for receiving and storing trust certificates issued by the certificate generator"]**;

(3) a code verifier for verifying that a particular player application is certified as a trusted application before digital content is transmitted to said particular player application **[i.e., referring to Figure 1D, the End-User Device(s) 109, that is "a code verifier", verifies the copy/play code before allowing the de-**

scrambling of the Content 113 and the execution of the play or copy (column 24, lines 3-7)]; and

(4) an authenticator for receiving requests, using an extension mechanism defined by the applications, to verify that a player application that requests protected content has been authorized by the verification system to access the requested, protected content **[i.e., referring to Figure 1D, a SC (secure container) is cryptographic carrier of information that uses cryptographic encryption, digital signatures and digital certificates to provide protection against unauthorized interception and modification of the electronic information or Content 113. It also allows for the authenticity verification, that is "an authenticator", of the electronic data (column 25, lines 10-15)].**

b. *Referring to claim 15:*

i. Hurtado further teaches:

(1) wherein the code verifier is responsible for launching the player application and verifying the identity and integrity of the code using the information in the trust certificate before launching the application; the launch procedure returning process identification information, which the code verifier records internally; the authenticator communicating the same or other process identification information concerning its own process, which it obtains from system service calls, to the code verifier at the time the application requests: content from the authenticator; the code verifier matching this process identification information against the process identification information it recorded; the code verifier returning a code indicating whether the process was verified or not **[i.e., referring to Figures 1A-1D, the control of Content usage is enabled through the End-User Player Application 195 running on an End-User Device(s). The application embeds a digital code in every copy of the Content that defines the allowable number of secondary copies and play backs. Digital watermarking technology is used to generate the digital code, to keep it hidden from other End-User Player Application 195, and to make it resistant to alteration attempts. In addition, a Secure Container (SC) is a structure that consists of several parts which together define a unit of Content 113 or a portion of a**

transaction, and which also define related information such as Usage Conditions, metadata, and encryption methods. SC(s) are designed in such a way that the integrity, completeness, and authenticity of the information can be verified. Some of the information in SC(s) may be encrypted so that it can only be accessed after proper authorization has been obtained (column 27, lines 27-36)].

c. *Referring to claim 16:*

i. This claim has limitations that is similar to those of claim 15, thus it is rejected with the same rationale applied against claim 15 above.

d. *Referring to claim 17:*

i. Hurtado further teaches:

(1) wherein the trust certificate includes: a program identifier identifying said one of the applications; a property name identifying an attribute certified by the trust certificate; a code digest of the one application; a digital signature containing a secret key of the application certifier; and a certifier identification containing a public key of the application certifier **[i.e., referring to Figure 1D, Secure Containers are used to distribute encrypted content and information among the system components. A SC is a cryptographic carrier of information or content that uses encryption, digital signatures, and digital certificates to provide protection against unauthorized interception or modification of electronic information and content. It also allows for the verification of the authenticity and integrity of the Digital Content. Furthermore, the system receives from the clearing house, a secure container encrypted using the encrypting key of the end user system containing the decrypting key for decrypting at least part of the previously encrypted content stored on the computer readable medium as permitted; and playing at least part of the previously encrypted content by decrypting the secure container using the encrypting key of the end user system to access the decrypting key for decrypting at least part of the encrypted content (column 10, lines 8-14). In addition, In the Secure Digital Content Electronic Distribution System 100, symmetric keys and other small data pieces are encrypted using public keys. Public key algorithms use two keys. The two keys are**

mathematically related so that data encrypted with one key can only be decrypted with the other key. The owner of the keys keeps one key private (private key) and publicly distributes the second key (public key) (column 16, lines 20-26)].

e. *Referring to claims 18 and 20:*

i. These claims have limitations that is similar to those of claim 14, thus they are rejected with the same rationale applied against claim 14 above.

f. *Referring to claims 19 and 21:*

i. These claims have limitations that is similar to those of claim 17, thus they are rejected with the same rationale applied against claim 17 above.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hurtado et al (US 6,611, 812 B2), and further in view of Vandergeest (US 6,247,127 B1).

a. *Referring to claim 1:*

i. Hurtado teaches:

(1) a verification system to validate the integrity of the player applications **[i.e., referring to Figure 1C, the Clearinghouse(s) 105 provides the licensing authorization and record keeping for all transactions that relate to the sale and/or permitted use of the Content 113 encrypted in a SC. When the Clearinghouse(s) 105 receives a request for a decryption key for the Content 113 from an intermediate or End-User(s), the Clearinghouse(s) 105, that is "a verification system", validates the integrity and authenticity of the information in the request; verifies that the request was authorized by an Electronic Digital Content Store(s) or Content Provider(s) 101; and verifies that the requested usage**

complies with the content Usage Conditions as defined by the Content Provider(s) 101 (column 13, lines 44-54)];

(2) a trusted content handler to decrypt content and to transmit the decrypted content to the player applications, using an extension mechanism defined by the application, and to enforce usage rights associated with the content **[i.e., referring to Figure 1D, the system receives from the clearing house, a secure container encrypted using the encrypting key of the end user system, that is "a trusted content handler", containing the decrypting key for decrypting at least part of the previously encrypted content stored on the computer readable medium as permitted; and playing at least part of the previously encrypted content by decrypting the secure container using the encrypting key of the end user system to access the decrypting key for decrypting at least part of the encrypted content (column 6, lines 6-14)];** and

(3) a user interface control module to ensure that the user interaction with the player applications does not violate the usage rights **[i.e., referring to Figure 1B, the Secure Digital Content Electronic Distribution System 100 provides the ability to handle retransmissions of Content 113. This is typically performed by a Customer Service Interface 184. Electronic Digital Content Store(s) 103 provides a user interface (that is "to ensure that users of the player applications are not exposed to actions that violate the usage rights") that the End-User(s) can step through in order to initiate a retransmission (column 50, lines 66-67 through column 51, lines 1-4)];**

(4) wherein components of the verification system, the trusted content handler, and user interface control module of the digital rights management system operate independently from the player application and reside locally in an end-user device having said player applications **[i.e., referring to Figure 1C, The Clearinghouse(s) 105 is responsible for the rights management functions of the Secure Digital Content Electronic Distribution System 100. Clearinghouse(s) 105 functions include enablement of Electronic Digital Content Store(s) 103, verification of rights to Content 113, integrity and authenticity**

validation of the buying transaction and related information, distribution of Content encryption keys or Symmetric Keys 623 to End-User Device(s) 109, tracking the distribution of those keys, and reporting of transaction summaries to Electronic Digital Content Store(s) 103 and Content Provider(s) 101 (column 45, lines 18-28)].

ii. Although Hurtado does not explicitly mention the off-line secure communications and/or operation independently from the player application, Vandergeest teaches:

(1) The secure information includes the certificates of end-users, or targeted communication entities. While the off-line end-user may receive the certificates for all other end-users of the system, typically, the off-line end-user will only request the certificates of end-users of interest, i.e., ones that will be involved in a secure communication with the off-line end-user. The secure information may further include cross-certificates 38, an authority revocation list 38, and a certificate revocation list 40. The off-line end-user verifies the secure information by comparing a time stamp of the security information with a validity period, which is based on the frequency at which the revocation lists 38 and 40 are updated. Thus if the revocation list 38 and 40 are updated daily, the validity period is 24 hours. The off-line end-user may further verify the security information by ensuring that a trust party (e.g., a trusted certification authority) signed the security information and the trusted party is not identified on the authority revocation list. The off-line end-user may still further verify the security information by determining that certificate of the at least one targeted communication is not on the certificate revocation list. The off-line end-user may even further verify the security information by ensuring that appropriate key usage, i.e., encryption keys are used for encryption purposes and verification keys are used for verification purposes. The off-line end-user may still even further verify the security information by ensuring policy compliance regarding the security information and messages based thereon **(column 4, lines 45-66).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include the off-line verification in Hurtado for providing off-line secure communication **(column 2, lines 51-52 of Vandergeest).**

iv. The ordinary skilled person would have been motivated to:

(1) include the off-line verification to allow end-users to go off-line from a security information repository (e.g., a directory, a certification authority, or a server), and confidently participate in secure communications. As such, an end-user, while off-line, may securely and in a trustworthy manner, read encrypted e-mail messages, prepare secure outgoing messages, access encryption protected folders, etc **(column 3, lines 3-9 of Vandergeest).**

b. *Referring to claim 2:*

i. Hurtado further teaches:

(1) wherein the verification system includes an off line verifier to verify that the player applications have certain properties, and to issue trust certificates to verify that the player applications have said properties **[i.e., in the Secure Digital Content Electronic Distribution System 100, the Clearinghouse(s) 105 has the option of issuing certificates to the Electronic Digital Content Store(s) 163. This allows the End-User Device(s) 109 to independently verify (this means "an off line verifier") that the Electronic Digital Content Store(s) 103 have been authorized by the Secure Digital Content Electronic Distribution System 100 (column 17, lines 42-49)].**

c. *Referring to claim 3:*

i. Hurtado further teaches:

(1) wherein the verification system further includes a verifying launcher for verifying that a particular player application is certified as a trusted application before digital content is transmitted to said particular player application **[i.e., referring to Figure 1C, Content Provider(s) 101 and Electronic Digital Content Store(s) 103 can request transaction reports from the Clearinghouse(s) 105 via a Payment Verification Interface 183 (wherein" a verifying launcher for verifying that a particular player application is certified as a trusted application before digital content is transmitted to said particular player application" is considered**

to include in this verification interface 183) so they can reconcile their own transaction databases with the information logged by the Clearinghouse(s) 105. The Clearinghouse(s) 105 can also provide periodic reports to the Content Provider(s) 101 and Electronic Digital Content Store(s) 103. The Clearinghouse(s) 105 defines a secure electronic interface which allows Content Provider(s) 101 and Electronic Digital Content Store(s) 103 to request and receive reports. The Report Request SC(s) includes a certificate that was assigned by the Clearinghouse(s) 105 to the entity initiating the request. The Clearinghouse(s) 105 uses the certificate and the SC's digital signature to verify that the request originated from an authorized entity (column 50, lines 1-16)].

d. *Referring to claim 4:*

i. Hurtado further teaches:

(1) wherein the player applications request protected content, and the trusted content handler includes an authenticator to verify that a player application that requests protected content has been authorized by the verification system to access the requested, protected content **[i.e., referring to Figure 1D, a SC (secure container) is cryptographic carrier of information that uses cryptographic encryption, digital signatures and digital certificates to provide protection against unauthorized interception and modification of the electronic information or Content 113. It also allows for the authenticity verification, that is "an authenticator", of the electronic data (column 25, lines 10-15)].**

e. *Referring to claim 5:*

i. Hurtado further teaches:

(1) wherein a user interface control module traps user interface related messages generated as a result of user interactions with player applications, blocks messages that lead to usage rights violations, and passes through other messages to the player applications **[i.e., referring to Figure 1B, Electronic Digital Content Store(s) 103 provides a user interface, which could "traps user interface related messages generated as a result of user interactions with player**

applications, blocks messages that lead to usage rights violations, and passes through other messages to the player applications" (column 51, lines 2-3)].

f. *Referring to claims 6 and 10:*

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

g. *Referring to claims 7 and 11:*

i. These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

h. *Referring to claims 8 and 12:*

i. These claims have limitations that is similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

i. *Referring to claims 9 and 13:*

i. These claims have limitations that is similar to those of claim 4, thus they are rejected with the same rationale applied against claim 4 above.

Response to Argument

5. Applicant's arguments filed July 06, 2004 have been fully considered but they are not persuasive.

Applicant argues that:

Moreover, with respect to the rejection of independent Claims 14, 18 and 20, as in the rejection of Claims 1, 6 and 10, the Examiner's reliance upon Hurtado is misplaced. These claims are directed to the details of the verification system and off-line process for validating a predefined property of the off-the-shelf player application, e.g., verifying a digest of the player application to ensure that it has not been modified.

Examiner maintains that:

Hurtado does teach the claimed subject matter as set forth in independent claims 14, 18, and 20. Hurtado further teaches in the Secure Digital Content Electronic Distribution System 100, the Clearinghouse(s) 105 has the option of issuing certificates to the Electronic Digital Content Store(s) 163. This allows the End-User Device(s) 109 to independently verify (this means "an off line verifier") that the Electronic Digital Content Store(s) 103 have been authorized by the Secure Digital Content Electronic

Distribution System 100 (column 17, lines 42-49). Furthermore, the phrase "off-line process for validating a predefined property of the off-the-shelf player application, e.g., verifying a digest of the player application to ensure that it has not been modified" that applicant uses to argue does not even read into the claimed language as set forth in independent claims 14, 18, and 20.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 21[illegible]